**System and Method For Secure Unidirectional Messaging**

**(A-70558/RMA)**

**WE CLAIM:**

1. A computer program product for use in conjunction with a computer system having a server and a client, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism, comprising: a program module that directs the computer system and/or components thereof including at least one or the client or server, to function in a specified manner to provide message communications, the message communications occurring in a computer system hardware architecture neutral and operating system neutral and network transport protocol neutral manner for secure unidirectional messaging, the program module including instructions for:

A. extracting, by the sender, an appropriate public key and matching destination address of a Recipient from a storage means that is trusted and has been verified;

B. extracting, by the sender, the sender's own private signing key and certificate chain from a trusted storage means;

C. passing, by the sender, that extracted public key and matching destination address and private signing key and certificate chain information, and the data of the message along with the Recipient's public enveloping key, and a fresh random data encryption key and fresh random OAEP padding seed to the Signed-Inside-Enveloped-Data cryptographic primitive to construct a secure unidirectional message;

D. sending, by the sender, the constructed secure unidirectional message;

E. receiving, by the Recipient, the message;

F. extracting, by the Recipient, its own private key from a secure storage means and decrypting the public key encryption;

G. extracting, by the Recipient, the data encryption key, and decrypting the data which is digitally signed; and

H. verifying the signature of the data and the certificate chain of the Sender;

I. wherein this is done using the same cryptographic primitive that is the same as the cryptographic primitive used with at least a secure session protocol.

2. A hardware architecture neutral and operating system neutral and network transport neutral method for secure unidirectional messaging using less software code and network bandwidth than conventional systems, said method comprising:

A. extracting, by the sender, an appropriate public key and matching destination address of a Recipient from a storage means that is trusted and has been verified;

B. extracting, by the sender, the sender's own private signing key and certificate chain from a trusted storage means;

C. passing, by the sender, that extracted public key and matching destination address and private signing key and certificate chain information, and the data of the message along with the Recipient's

public enveloping key, and a fresh random data encryption key and fresh random OAEP padding seed to the Signed-Inside-Enveloped-Data cryptographic primitive to construct a secure unidirectional message;

D. sending, by the sender, the constructed secure unidirectional message;

E. receiving, by the Recipient, the message;

F. extracting, by the Recipient, its own private key from a secure storage means and decrypting the public key encryption;

G. extracting, by the Recipient, the data encryption key, and decrypting the data which is digitally signed; and

H. verifying the signature of the data and the certificate chain of the Sender;

I. wherein this is done using the same cryptographic primitive that is the same as the cryptographic primitive used with at least a secure session protocol.

3. The method in Claim 2, wherein said appropriate public key comprises an RSA based public key.

4. The method in Claim 2, wherein said matching destination address is selected from the set consisting of an e-mail address and a URL.

5. The method in Claim 2, wherein said storage means is trusted and has been previously verified using a digital signature or cryptographic checksum.

6. The method in Claim 2, wherein said digital signature provides verification with a trusted public key.

7. The method in Claim 2, wherein said cryptographic checksum provides verification with a trusted key derived from a Master Key, a Session Key, or a Message Key.

8. The method in Claim 2, wherein the storage means is selected from the group consisting of a Compact Certificate, a chain of Compact Certificates leading to a trusted root public key, or combinations thereof.

9. The method in Claim 2, wherein the storage means is a previously received Storymail story enabled message that was securely received and verified by mechanisms that are trusted for that kind of message.

10. The method in Claim 2, wherein the storage means is any conventional e-mail message or web page which the Sender trusts that has been copied into the Sender's messaging platform memory via mechanisms that the Sender trusts.

11. The method in Claim 10, wherein the messaging platform is a messaging platform selected from the set consisting of: a computer, a server, a PDA, a telephone, an appliance, an information appliance, a pager, or any other device supporting such messaging.

12. The method in Claim 2, wherein the OAEP padding seed and the data encryption key are different values.

13. The method in Claim 2, wherein the OAEP padding seed and the data encryption key are the same value to avoid the overhead of generating multiple random values.

14. The method in Claim 2, wherein the Sender's private key and certificate chain comprise fixed values shared among a plurality of Senders.

15. The method in Claim 2, wherein the Sender's private key and certificate chain fixed values are widely known.

16. The method in Claim 2, wherein the Sender's private key and certificate chain fixed values are not widely known and the Sender's software employs mechanisms to make it difficult to discover these values through a process of reverse engineering.

17. A method for secure unidirectional messaging from a sender to a recipient, said method comprising:

obtaining, by the sender, a public key and destination address of a message recipient and the sender's own private signing key and certificate chain from one or more trusted source;

passing, by the sender, the extracted public key and matching destination address and private signing key and certificate chain information, and the data of an intended message along with the recipient's public enveloping key and a random data encryption key and random padding seed to a cryptographic primitive; and

constructing, by the sender, a secure unidirectional message there from.

18. The method of claim 17, further comprising: sending, by the sender, the constructed secure unidirectional message to the recipient.

19. The method of claim 18, further comprising:

receiving the secure unidirectional message by the recipient;

extracting, by the Recipient, the recipient's own private key from a secure source and decrypting the public key encryption, and the data encryption key and decrypting the data which is digitally signed; and

verifying the signature of the data and the certificate chain of the sender.

20. The method of claim 18, wherein said message is an e-mail message.

21. The method of claim 18, wherein said message is a Storymail story message.

22. The method of claim 18, wherein the trusted source or storage means comprises a Compact Certificate as explained earlier, or chain of Compact Certificates leading to a trusted root public key.